Allegato Tecnico di Compliance e Sicurezza – Accordo Quadro RTRT4 - Azienda Regionale Diritto allo Studio Universitario

Emesso da: CE.E.PS/C Data: 30.11.2022

REDATTO:	CE.E.PS/C
VERIFICATO/APPROVATO	CE.E.PS.CGK
LISTA DI DISTRIBUZIONE:	il presente documento viene distribuito alla funzione di Vendita interessata, al Cliente e, in caso di accettazione, alla funzione Procurement ed ai fornitori
TIPO ATCS	**PLURI-FORNITORE**

Il presente documento è stato redatto in coerenza con il Codice Etico e di Condotta ed il Modello Organizzativo 231 del Gruppo Telecom Italia

TIM S.p.A.

Sede legale: Via Gaetano Negri, 1 - 20123 Milano
Sede secondaria e Direzione Generale: Corso d'Italia, 41 - 00198 Roma
Casella PEC: telecomitalia@pec.telecomitalia.it

Codice Fiscale/P. IVA e Iscrizione al Registro delle Imprese di Milano: 00488410010
Iscrizione al Registro A.E.E. IT08020000000799
Capitale Sociale € 11.677.002.855,10 interamente versato

Allegato Tecnico di Compliance e Sicurezza – Accordo Quadro RTRT4 - Azienda Regionale Diritto allo Studio Universitario

Emesso da: CE.E.PS/C Data: 30.11.2022

ALLEGATO TECNICO DI COMPLIANCE E SICUREZZA

Di seguito sono trattati i seguenti aspetti del GDPR per i servizi IT oggetto del contratto:

- l'elenco dei trattamenti affidati a TIM e ai suoi fornitori nel ruolo di controller o processor
- il tipo dato
- un insieme di requisiti (intesi come misure di sicurezza), laddove applicabili, definite dalla policy di Compliance TIM, da valutare prima di svolgere il trattamento in coerenza ai principi della privacy by design e by default.

Anagrafica Cliente Titolare del Trattamento

Cliente: Ragione Sociale	**Azienda Regionale Diritto allo Studio Universitario**
Referente Cliente ("Referente DPO se disponibile" o referente tecnico)	
Nome Referente	Mario
Cognome Referente	Arcella
Email	dpo@dsu.toscana.it.
Cellulare	
Telefono	

Anagrafica Responsabili del trattamento

Anagrafica TIM

Fornitore	
Fornitore: Ragione Sociale	Tim Spa
Codice Fiscale /Partita IVA	00488410010
Rappresentante per Fornitori extra UE	
Mail Rappresentante per Fornitori extra UE	

Allegato Tecnico di Compliance e Sicurezza – Accordo Quadro RTRT4 - Azienda Regionale Diritto allo Studio Universitario

Emesso da: CE.E.PS/C Data: 30.11.2022

Anagrafica OpenSymbol

Fornitore	
Fornitore: Ragione Sociale	Opensymbol SRL a socio unico
Codice Fiscale /Partita IVA	03184500241
Rappresentante per Fornitori extra UE	NA
Mail Rappresentante per Fornitori extra UE	NA

Anagrafica Telsy

Fornitore	
Fornitore: Ragione Sociale	Telsy SpA con unico socio Gruppo TIM
Codice Fiscale /Partita IVA	00737690016
Rappresentante per Fornitori extra UE	
Mail Rappresentante per Fornitori extra UE	

Anagrafica Maticmind

Fornitore	
Fornitore: Ragione Sociale	Maticmind S.p.A.
Codice Fiscale /Partita IVA	05032840968
Rappresentante per Fornitori extra UE	
Mail Rappresentante per Fornitori extra UE	

Anagrafica Sime Telecomunicazioni

Fornitore	
Fornitore: Ragione Sociale	Sime Telecomunicazioni

Allegato Tecnico di Compliance e Sicurezza – Accordo Quadro RTRT4 - Azienda Regionale Diritto allo Studio Universitario

Emesso da: CE.E.PS/C Data: 30.11.2022

Codice Fiscale /Partita IVA	06370160480
Rappresentante per Fornitori extra UE	
Mail Rappresentante per Fornitori extra UE	

1. Anagrafica Soluzioni/Piattaforme, Tipo dato, Trattamenti e Responsabili dei Trattamenti

Soluzioni per le quali TIM è Titolare dei Trattamenti
SOLUZIONI DI Trasmissione DATI SINFONIA Custom

➢ Soluzioni per le quali OpenSymbol è Responsabile del Trattamento

Nome Soluzione (Tipologia soluzione Standard, Personalizzata o Custom)	**Tipologia Dati (Perimetro di Compliance)**	**Categorie di Trattamenti - Responsabili dei Trattamenti**		**Ubicazione piattaforma**
PORTALE WEB DI GESTIONE DELLA FORNITURA RTRT4	Dati Personali Comuni Perimetro Portali Web Perimetro PA (Misure Agid)			DC Noovle (TIM Hosting Evoluto)
		Gestione sistemistica infrastrutturale	Noovle	
		Gestione sistemistica	Noovle	
		Storage	Noovle	
		Gestione middleware	OpenSymbol	
		Gestione database	OpenSymbol	
		Gestione applicativa	OpenSymbol	
		Raccolta ed analisi dei security log (gestione piattaforme di correlazione)	Noovle	
		Backup	Noovle	

Responsabile dello sviluppo software	**Nome Soluzione**
OpenSymbol	SEP

Allegato Tecnico di Compliance e Sicurezza – Accordo Quadro RTRT4 - Azienda Regionale Diritto allo Studio Universitario

Emesso da: CE.E.PS/C Data: 30.11.2022

➢ Soluzioni per le quali Telsy e Maticmind sono Responsabili del Trattamento

Nome Soluzione	Tipologia Dati (Perimetro di Compliance)	Categorie di Trattamenti	Responsabili dei Trattamenti	Ubicazione piattaforma e dati trattati
SERVIZI DI SICUREZZA (SSONP e SSCEN) TIM Area Protection Fast	Dati Personali Comuni Perimetro PA (Misure Agid)	Gestione sistemistica infrastrutturale	Telsy (SOC)	Onsite (Cliente) per l'apparato di Sicurezza (firewall): per i servizi SSONP DC Noovle: per i servizi SSCEN e per la piattaforma di gestione e collection dei security log[1]/audit log (Log di Accesso[2])
		Gestione sistemistica e raccolta, consultazione e conservazione dei security log (gestione FW)	Telsy (SOC)	
		Storage	Telsy (SOC)	
		Gestione middleware	Telsy (SOC)	
		Gestione applicativa	Telsy (SOC)	
		Backup configurazioni dei Firewall	Telsy (SOC)	
		Gestione sistemistica dell'apparato durante la fase iniziale di configurazione e installazione presso la sede del Cliente o presso Data Center Noovle	MaticMind	
		Manutenzione hardware	MaticMind	

➢ Soluzioni per le quali Simetel è Responsabile del Trattamento

[1] l'insieme delle registrazioni relative alle violazioni delle policy di sicurezza implementate sulla Piattaforma e che consentono di effettuare un'indagine in merito alla causa della violazione;

[2] le registrazioni che garantiscono la completa tracciabilità di tutti gli accessi (Login) e di tutte le disconnessioni (Logout) eseguite dalle utenze di amministratore di sistema che hanno avuto accesso a ciascun sistema o Piattaforma;

Allegato Tecnico di Compliance e Sicurezza – Accordo Quadro RTRT4 - Azienda Regionale Diritto allo Studio Universitario

Emesso da: CE.E.PS/C Data: 30.11.2022

Nome Soluzione	Tipologia Dati (Perimetro di Compliance)	Categorie di Trattamenti	Responsabili dei Trattamenti	Ubicazione piattaforma e dati trattati
Servizio di Presidio	Dati Personali Comuni Perimetro PA (Misure Agid)	Presidio	Simetel	Sede TIM

Stati extra UE dove trasferiti dati	Rappresentante per clienti extra UE

Presenza di servizi/trattamenti in cogestione col cliente	Nome servizio/trattamenti in cogestione col cliente
NO	

2. Allegato Tecnico "Requisiti di sicurezza dei dati della piattaforma"

Di seguito si riportano i requisiti di sicurezza suddivisi per tipologia di dato e per perimetro di compliance con il dettaglio dell'effettiva applicazione di ciascuno di essi da parte dei fornitori Telsy e Opensymbol Responsabili del Trattamento.

Per Maticmind e Simetel, non svolgendo alcuna attività di gestione sistemistica e/o applicativa su componenti della soluzione,ma attività rispettivamente di manutenzione di apparati di sicurezza e di presidio, non risultano applicabili i requisiti di sicurezza.

I trattamenti effettuati da Noovle nell'ambito dei TIM servizi standard Hosting Evoluto sono certificati compliant al GDPR e non oggetto del presente ATCS.

GLOSSARIO: Nelle misure di sicurezza sono riferiti i seguenti ruoli:

- Gestori IT: Il Gestore è il responsabile della gestione tecnica (sviluppo, esercizio, manutenzione, aggiornamento, ecc.) di un sistema ICT
- Addetti IT: I soggetti autorizzati da società del gruppo TIM al trattamento, destinatari di utenze di accesso amministrativo, preposte alla gestione sistemistica o applicativa della piattaforma. Possono essere interni (dipendenti di TIM) o esterni (dipendenti del Partner o del Fornitore)
- End-User Autorizzati: Utilizzatori finali del servizio IT (ad es. dipendenti del Cliente) caratterizzati da utenze di accesso all'Applicativo, autorizzati da parte del titolare, cioè il Cliente business a compiere

operazioni di trattamento sui dati gestiti dall'applicativo. Possono assumere anche il ruolo di Amministratore dell'Applicativo.

- End-User interessati: Rappresentano i soggetti cui si riferiscono i dati personali gestiti dall'applicativo e che possono eventualmente essere anche utilizzatori finali del servizio IT; in tal caso sono assegnatari di utenze di accesso all'Applicativo di tipo non amministrativo, con profili ristretti ai dati di propria competenza

2.1. Perimetro “231/reati informatici” e/o Perimetro Dati Personali Comuni

Questo perimetro è composto da piattaforme che:

- non trattano dati personali. Il Modello Organizzativo e la relativa Policy TIM prevedono una rilevanza a medio rischio reato D.Lgs 231/01 – Reati informatici.
- trattano i Dati Personali “comuni”. «dato personale»: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.

Laddove applicabile, all’interno del testo requisito, è indicata la corrispondente misura minima Agid soddisfatta attraverso la nomenclatura ABSC (Agid Basic Security Controll), cioè con identificatore gerarchico a tre livelli x,y.z preceduti dalla lettera M per indicare la misura come minima (**[M].x.y.z**).

ID MISURA	Categoria MIMIP	Testo requisito	Telsy	OpenSymbol
CdC-ICT.003.1	Canali di comunicazione	Le piattaforme e gli apparati in DC TIM sono protetti da meccanismi per la rilevazione del traffico anomalo (es. sonde di sicurezza) in grado di rilevare sia attacchi provenienti dalla rete di gruppo TIM verso le piattaforme, sia attacchi uscenti dalle piattaforme (qualora gestite da personale di TIM) verso la rete pubblica.	Applicato	NA la piattaforma è su hosting evoluto di Opensymbol ma in DC Noovle
CdC-ICT.006.1	Canali di comunicazione	Sulle piattaforme al momento della messa in produzione del sistema, viene svolta una attività di vulnerability assessment (ingaggiando le funzioni preposte) con una metodologia di tipo non intrusivo e/o con l’utilizzo di tool automatici. La possibilità di effettuare l’attività di VA è valutata e documentata al momento della messa in produzione della piattaforma, in funzione delle possibili criticità emerse durante la	Applicato	NA la piattaforma è su hosting evoluto di Opensymbol ma in DC Noovle

Allegato Tecnico di Compliance e Sicurezza – Accordo Quadro RTRT4 - Azienda Regionale Diritto allo Studio Universitario

Emesso da: CE.E.PS/C Data: 30.11.2022

ID MISURA	Categoria MIMIP	Testo requisito	Telsy	OpenSymbol
		fase collaudo. Qualora sulla piattaforma non sia stato svolto un VA in fase di rilascio della stessa in ambiente di esercizio, tale intervento dovrà essere pianificato dalle funzioni preposte. In ogni caso deve essere prevista la rivalutazione del VA in caso di modifiche significative della piattaforma ingaggiando le funzioni preposte.		
CdC-ICT.007.1	Canali di comunicazione	Sono previsti meccanismi di protezione perimetrale (es. Firewall) delle infrastrutture e dei sistemi. Tali meccanismi ispezionano e proteggono, laddove applicabile, almeno i 3 macro-flussi: 1. dalle reti interne TIM, cliente, fornitore verso la piattaforma; 2. dalla rete pubblica Internet verso la piattaforma; 3. dalla piattaforma verso la rete pubblica Internet.	Applicato	NA la piattaforma è su hosting evoluto di Opensymbol ma in DC Noovle
CdC-ICT.008.1	Canali di comunicazione	Sono adottate e documentate politiche di configurazione degli apparati di sicurezza (es. tipologie e direzione flussi attraverso Firewall, ecc.).	Applicato	NA la piattaforma è su hosting evoluto di Opensymbol ma in DC Noovle
CdC-ICT.009.1	Canali di comunicazione	Nel caso vengano utilizzati accessi in VPN ai sistemi è identificabile in forma nominativa l'utilizzatore di un dato indirizzo IP (ad esempio mediante VPN client-to-lan o meccanismi di client-authentication delle sessioni).	Applicato	Applicato

Allegato Tecnico di Compliance e Sicurezza – Accordo Quadro RTRT4 - Azienda Regionale Diritto allo Studio Universitario

Emesso da: CE.E.PS/C Data: 30.11.2022

ID MISURA	Categoria MIMIP	Testo requisito	Telsy	OpenSymbol
CoA-ICT.010.1	Controllo accessi	Quando il sistema utilizza la password come dispositivo di autenticazione, sono adottate misure per la protezione (ad es. cifratura) delle credenziali memorizzate a sistema (ad es. password sistemistiche ed applicative, certificati digitali). Devono inoltre essere previste misure di protezione della password (ad es. cifratura) anche quando transitano in rete e nel canale in fase di autenticazione (incluse le connessioni M2M). **[M] 5.11.1** **[M] 5.11.2**	Applicato	Applicato
PdE-ICT.010.1	Protezione degli elaboratori	La piattaforma, e le sue componenti, sviluppate internamente da TIM (o da un suo fornitore) sono dotate di software sviluppato secondo metodologie di sviluppo sicuro laddove è applicabile	Applicato	Applicato
AuL-ICT.008.1 AuL-ICT.008.2	Audit log	La piattaforma tramite cui è effettuato il trattamento di dati, o l'eventuale piattaforma centralizzata di Identity Management ad essa connessa, è configurata in maniera tale da: - produrre la registrazione degli accessi logici (Access Log), compresi i tentativi falliti di accesso, effettuati da parte degli Amministratori di Sistema Addetti IT interni ed esterni - conservare le registrazioni per un periodo di sei mesi a meno di analisi del rischio che prevedano fino a 12 mesi o accordi contrattuali specifici con il cliente che prevedano tempi superiori ai 6 mesi.	Applicato	Applicato

Allegato Tecnico di Compliance e Sicurezza – Accordo Quadro RTRT4 - Azienda Regionale Diritto allo Studio Universitario

Emesso da: CE.E.PS/C Data: 30.11.2022

ID MISURA	Categoria MIMIP	Testo requisito	Telsy	OpenSymbol
AuL-ICT.009.1	Audit log	Nel caso gli End User Autorizzati si configurino come Amministratori di Sistema Software, la piattaforma tramite cui è effettuato il trattamento di Dati Personali, o l'eventuale piattaforma centralizzata di Identity Management ad essa connessa è configurata in maniera tale da: - prevedere meccanismi di registrazione degli accessi logici (access log), compresi i tentativi falliti di accesso; - conservare le registrazioni per un periodo di sei mesi.	Applicato	Applicato
AuL-ICT.010.1 AuL-ICT.010.2	Audit log	E' garantita la completezza, l'immodificabilità e la possibilità di verificare l'integrità delle registrazioni dei log di accesso degli Addetti IT (ad es. tramite l'invio a sistemi di Log Collecting centralizzati).	Applicato	Applicato
AuL-ICT.011.1	Audit log	Nel caso gli End User Autorizzati si configurino come Amministratori di Sistema Software (accesso a livello del Sistema Operativo, del Data Base, dei middleware, di tutte le componenti infrastrutturali comprese le piattaforme di back up e di manutenzione dell'Applicativo), è garantita la completezza, l'immodificabilità e la possibilità di verificare l'integrità delle registrazioni dei log di accesso all'applicativo degli stessi.	Applicato	NA la piattaforma è su hosting evoluto di Opensymbol ma in DC Noovle
AuL-ICT.012.1 AuL-ICT.012.2	Audit log	La piattaforma tramite cui è effettuato il trattamento di dati, o l'eventuale piattaforma centralizzata di Identity Management ad essa connessa, è configurata in maniera tale da prevedere	Applicato	Applicato

Allegato Tecnico di Compliance e Sicurezza – Accordo Quadro RTRT4 - Azienda Regionale Diritto allo Studio Universitario

Emesso da: CE.E.PS/C Data: 30.11.2022

ID MISURA	Categoria MIMIP	Testo requisito	Telsy	OpenSymbol
		tecnologie di sincronizzazione al fine di mantenere allineata la data e l'ora associata agli accessi registrati nei log.		
AuL-ICT.013.1 AuL-ICT.013.2	Audit log	Le registrazioni dei log relativi agli accessi (access log) alla piattaforma degli Addetti IT includono le seguenti informazioni: - il sistema target e l'eventuale applicazione acceduta; - evento che ha generato il log (login, logout, failure login); - utenza, data e ora di inizio / fine connessione. **[M] 5.1.2**	Applicato	Applicato
AuL-ICT.014.1 AuL-ICT.014.2	Audit log	Nel caso gli End User Autorizzati si configurino come Amministratori di Sistema IT, le registrazioni dei log di accesso (access log) degli stessi all'applicativo includono le seguenti informazioni: - il sistema target e l'eventuale applicazione acceduta; - evento che ha generato il log (login, logout, failure login); - utenza, data e ora di inizio / fine connessione. **[M] 5.1.2**	Applicato	Applicato
Bck-ICT.002.1 Bck-ICT.002.2	Back-up	Al fine di garantire la disponibilità e l'integrità dei dati è prevista la definizione e l'esecuzione di procedure di backup con cadenza almeno settimanale per i dati di configurazione e per i dati del Cliente. **[M] 10.1.1** **[M] 10.3.1** **[M] 10.4.1**	Applicato	Applicato

Allegato Tecnico di Compliance e Sicurezza – Accordo Quadro RTRT4 - Azienda Regionale Diritto allo Studio Universitario

Emesso da: CE.E.PS/C Data: 30.11.2022

ID MISURA	Categoria MIMIP	Testo requisito	Telsy	OpenSymbol
CdA-ICT.002.1 CdA-ICT.002.2	Credenziali di autenticazione	Tutti i profili di accesso e le politiche di gestione delle utenze degli Addetti IT (interni ed esterni) delle piattaforme sono verificati e aggiornati. Tale verifica avviene con frequenza almeno annuale o comunque a seguito di eventi significativi (es. cambi organizzativi, evoluzioni di sistema, etc.). **[M] 5.1.1**	Applicato	Non applicabile in quanto la gestione delle credenziali viene ereditata, tramite collegamento sicuro, dall'LDAP di TIM che ne determina la validità e la relativa gerarchia (Ruoli e permessi) SEP gestisce poi il flusso di approvazione di un utente che faccia richiesta di accedere alla piattaforma a condizione che la validità dell'utente stesso sia confermata dall'LDAP di TIM
CdA-ICT.003.1 CdA-ICT.003.2	Credenziali di autenticazione	Il Gestore, o un suo delegato, autorizza le utenze degli Addetti IT all'accesso ai dati nella fase di creazione, modifica o monitoraggio (gestione credenziali di accesso). **[M] 5.2.1**	Applicato	Non applicabile in quanto la gestione delle credenziali viene ereditata, tramite collegamento sicuro, dall'LDAP di TIM che ne determina la validità e la relativa gerarchia (Ruoli e permessi) SEP gestisce poi il flusso di approvazione di un utente che faccia richiesta di accedere alla piattaforma a condizione che la validità

Allegato Tecnico di Compliance e Sicurezza – Accordo Quadro RTRT4 - Azienda Regionale Diritto allo Studio Universitario

Emesso da: CE.E.PS/C Data: 30.11.2022

ID MISURA	Categoria MIMIP	Testo requisito	Telsy	OpenSymbol
				dell'utente stesso sia confermata dall'LDAP di TIM
CdA-ICT.004.1 CdA-ICT.004.2	Credenziali di autenticazione	Gli amministratori di sistema sono stati formalmente nominati. **[M] 5.2.1**	Applicato	Applicato
CdA-ICT.005.1 CdA-ICT.005.2	Credenziali di autenticazione	Per una gestione delle credenziali di autenticazione, la piattaforma, o l'eventuale piattaforma centralizzata di Identity Management ad essa connessa, è configurata in modo tale da associare a ciascun utenza dedicata agli Addetti IT credenziali di autenticazione individuali (costituite da una User-ID e un dispositivo di autenticazione - ad es. password). La piattaforma, inoltre, deve prevedere all'accesso meccanismi automatici di verifica delle stesse. **[M] 5.10.2**	Applicato	Applicato
CdA-ICT.006.1 CdA-ICT.006.2	Credenziali di autenticazione	Per una gestione delle credenziali di autenticazione, la piattaforma, o l'eventuale piattaforma centralizzata di Identity Management ad essa connessa, è configurata in modo tale da associare a ciascun utenza dedicata agli End User Autorizzati credenziali di autenticazione individuali (costituite da una User-ID e un dispositivo di autenticazione - ad es. password). La piattaforma, inoltre, deve prevedere all'accesso meccanismi automatici di verifica delle stesse. **[M] 5.10.2**	Applicato	Applicato

Allegato Tecnico di Compliance e Sicurezza – Accordo Quadro RTRT4 - Azienda Regionale Diritto allo Studio Universitario

Emesso da: CE.E.PS/C Data: 30.11.2022

ID MISURA	Categoria MIMIP	Testo requisito	Telsy	OpenSymbol
		[M] 5.2.1		
CdA-ICT.007.1 CdA-ICT.007.2	Credenziali di autenticazione	La piattaforma, o l'eventuale piattaforma centralizzata di Identity Management ad essa connessa, prevede meccanismi automatici di verifica atti a impedire la riassegnazione di User-ID ad altri autorizzati neppure in tempi diversi. **[M] 5.10.2**	Applicato	Applicato
CdA-ICT.009.1 CdA-ICT.009.2	Credenziali di autenticazione	La piattaforma è configurata in modo tale che garantisca una soluzione tecnica o procedurale che consenta, in caso di cancellazione di utenze (assegnate ad Addetti IT), di risalire in maniera certa alla persona fisica assegnataria, in un dato periodo, dell'utenza in oggetto. Tali informazioni sono conservate per almeno un periodo di 60 mesi dalla cancellazione delle utenze. **[M] 5.10.2**	Applicato	Applicato
CdA-ICT.011.1 CdA-ICT.011.2	Credenziali di autenticazione	La piattaforma consente di associare le utenze degli Addetti IT ai profili rispettando i principi di "need to know" e "segregation of duties" **[M] 5.1.1** **[M] 5.1.2** **[M] 5.2.1**	Applicato	Applicato
CdA-ICT.012.1	Credenziali di autenticazione	L'applicativo è sviluppato in maniera tale da consentire la definizione di insiemi di profili di accesso per gli End User Autorizzati che garantiscano i principi di "need to know".	Applicato	Applicato
CdA-ICT.013.1 CdA-ICT.013.2	Credenziali di autenticazione	La piattaforma, o l'eventuale piattaforma centralizzata di Identity Management ad essa connessa deve essere configurata in maniera tale che effettui la verifica (almeno	Applicato	Applicato

Allegato Tecnico di Compliance e Sicurezza – Accordo Quadro RTRT4 - Azienda Regionale Diritto allo Studio Universitario

Emesso da: CE.E.PS/C Data: 30.11.2022

ID MISURA	Categoria MIMIP	Testo requisito	Telsy	OpenSymbol
		settimanale se eseguita tramite modalità automatiche o mensile per analisi procedurali), di tutte le utenze associate ad Addetti IT che hanno lasciato l'azienda al fine di cessare tempestivamente tutte le relative abilitazioni sulla piattaforma. **[M] 5.2.1**:		
CdA-ICT.014.1 CdA-ICT.014.2	Credenziali di autenticazione	Tutte le utenze degli Addetti IT sono sottoposte a rivalutazioni periodiche circa la sussistenza delle esigenze che ne hanno portato all'attivazione. In particolare le revisioni delle utenze devono essere previste con periodicità almeno annuale **[M] 5.1.1**	Applicato	Applicato
CdA-ICT.015.1 CdA-ICT.015.2	Credenziali di autenticazione	L'applicativo è sviluppato in maniera tale da prevedere meccanismi in grado di consentire l'estrazione delle informazioni necessarie alla verifica della corretta attribuzione delle credenziali di autenticazione e dei relativi profili di autorizzazione degli End User Autorizzati. **[M] 5.2.1**	Applicato	Applicato
CdA-ICT.018.1	Credenziali di autenticazione	La piattaforma consente la sospensione delle utenze inattive degli End User Autorizzati a valle di periodi di inattività pari o maggiori a 6 mesi, salvo le utenze per le quali è stata preventivamente richiesta ed autorizzata una deroga sulla base di una necessità operativa.	Applicato	Applicato
CdA-ICT.019.1 CdA-ICT.019.2	Credenziali di autenticazione	Il gruppo in carico della creazione e della assegnazione delle credenziali di autenticazione agli Addetti IT richiedenti risulta essere nominato e	Applicato	Applicato

Allegato Tecnico di Compliance e Sicurezza – Accordo Quadro RTRT4 - Azienda Regionale Diritto allo Studio Universitario

Emesso da: CE.E.PS/C Data: 30.11.2022

ID MISURA	Categoria MIMIP	Testo requisito	Telsy	OpenSymbol
		costituito da un numero circoscritto di Addetti IT preventivamente individuati. **[M] 5.2.1**		
CdA-ICT.020.1 CdA-ICT.020.2	Credenziali di autenticazione	E' precluso l'utilizzo di utenze di Sistema su processi automatici (ad esempio le utenze di Sistema non sono utilizzate come utenze Machine to Machine).	Applicato	Non applicato perché non previsto contrattualmente
CdA-ICT.021.1 CdA-ICT.021.2	Credenziali di autenticazione	E' precluso l'utilizzo di utenze di sistema e M2M da parte di persone fisiche, ad eccezione di attività saltuarie (es. gestione emergenze).	Applicato	Non applicato perché non previsto contrattualmente
CdA-ICT.022.1 CdA-ICT.022.2	Credenziali di autenticazione	La piattaforma, o l'eventuale piattaforma centralizzata di Identity Management ad essa connessa, è configurata in maniera tale che le utenze di sistema non nominali (comprese le M2M) devono essere comunque assegnate (in termini di responsabilità) ad una persona fisica, tipicamente un Responsabile di esercizio o un suo delegato. **[M] 5.10.2**	Applicato	Non applicato perché non previsto contrattualmente
CdA-ICT.023.1 CdA-ICT.023.2	Credenziali di autenticazione	Gli addetti IT a cui sono assegnate utenze deputate allo svolgimento di attività di sicurezza relative alla protezione dei sistemi (per es. configurazione regole FW o monitoraggio allarmi di sicurezza) sono distinti, a livello di singolo individuo, dagli altri addetti IT degli stessi sistemi. La separazione, a livello di singolo individuo, è applicata anche tra chi configura gli strumenti di sicurezza (es. FW o IDS) e chi svolge attività di verifica della sicurezza (es. vulnerability assessment). **[M] 5.1.1**	Applicato	Applicato

Allegato Tecnico di Compliance e Sicurezza – Accordo Quadro RTRT4 - Azienda Regionale Diritto allo Studio Universitario

Emesso da: CE.E.PS/C Data: 30.11.2022

ID MISURA	Categoria MIMIP	Testo requisito	Telsy	OpenSymbol
CdA-ICT.024.1 CdA-ICT.024.2	Credenziali di autenticazione	Gli addetti IT a cui sono assegnate utenze deputate alla gestione dei file di log sono distinti, a livello individuale, dagli altri addetti IT dello stesso sistema. Nel caso di sistema di supporto dedicato alla gestione dei file di log non sussiste vincolo di incompatibilità con le attività di gestione sistemistica / applicativa del sistema stesso.	Applicato	Non applicabile in quanto la gestione delle credenziali viene ereditata, tramite collegamento sicuro, dall'LDAP di TIM che ne determina la validità e la relativa gerarchia (Ruoli e permessi) SEP gestisce poi il flusso di approvazione di un utente che faccia richiesta di accedere alla piattaforma a condizione che la validità dell'utente stesso sia confermata dall'LDAP di TIM
CdA-ICT.025.1 CdA-ICT.025.2	Credenziali di autenticazione	Per una gestione delle modalità di accesso dedicate a ciascun Addetto IT interno ed esterno, la piattaforma, o l'eventuale piattaforma centralizzata di Identity Management ad essa connessa, è configurata in maniera tale che quando il sistema utilizza la password come dispositivo di autenticazione, essa effettui controlli automatici volti a garantire che la password risponda alle caratteristiche previste dalle vigenti policy aziendali. **[M] 5.11.1** **[M] 5.7.4**	Applicato	Applicato

Allegato Tecnico di Compliance e Sicurezza – Accordo Quadro RTRT4 - Azienda Regionale Diritto allo Studio Universitario

Emesso da: CE.E.PS/C Data: 30.11.2022

ID MISURA	Categoria MIMIP	Testo requisito	Telsy	OpenSymbol
CdA-ICT.026.1	Credenziali di autenticazione	La piattaforma consente la sospensione delle utenze inattive degli Addetti IT a valle di periodi di inattività pari o maggiori a 6 mesi, (salvo le utenze preventivamente autorizzate per soli scopi di gestione tecnica per le quali sia stata concessa una deroga da parte del Gestore IT o suoi delegati). Nel caso di infattibilità tecnica il controllo può essere di tipo procedurale, con frequenza almeno mensile, garantendo comunque la sospensione trascorsi 6 mesi di inattività.	Applicato	Applicato
CdC-ICT.002.1 CdC-ICT.002.2	Canali di comunicazione	E' prevista l'adozione di apparati hardware e software (ad es. firewall) in grado di contrastare tentativi di accesso non autorizzato da reti dati pubbliche (Internet) al fine di rispettare i livelli di isolamento e protezione dei dati trattati dalla piattaforma stessa. **[M] 8.1.2**	Applicato	NA la piattaforma è su hosting evoluto di Opensymbol ma in DC Noovle
CdC-ICT.012.1 CdC-ICT.012.2	Canali di comunicazione	Per tutti i sistemi in perimetro per i quali sia consentito l'accesso al sistema da parte di entità terze/esterne all'azienda (fornitori), è garantita, salvo diversa indicazione, la sicurezza dei dati scambiati verso l'esterno (es. canali con protocolli sicuri, meccanismi di cifratura).	Applicato	Applicato
CoA-ICT.004.1 CoA-ICT.004.2	Controllo accessi	La piattaforma, o l'eventuale piattaforma centralizzata di Identity Management ad essa connessa prevede meccanismi automatici di verifica atti a garantire i requisiti di robustezza delle credenziali di autenticazione. A tal fine deve essere prevista	Applicato	Non applicabile in quanto la gestione delle credenziali viene ereditata, tramite collegamento sicuro, dall'LDAP di TIM che ne

Allegato Tecnico di Compliance e Sicurezza – Accordo Quadro RTRT4 - Azienda Regionale Diritto allo Studio Universitario

Emesso da: CE.E.PS/C Data: 30.11.2022

ID MISURA	Categoria MIMIP	Testo requisito	Telsy	OpenSymbol
		l'implementazione di controlli automatici volti a garantire che le credenziali di autenticazione (per es. password) rispondano alle caratteristiche di sicurezza previste. In particolare la password deve prevedere: • lunghezza minima pari a 8 caratteri o al massimo permesso dal sistema; • complessità (la password deve essere costituita da caratteri diversi per tipologia quali lettere, numeri, simboli speciali) • diversità dalle precedenti 4 password (password history); In caso di soluzione/piattaforma destinata alla Pubblica Amministrazione (AgID ABSC Minimo): • se l'autenticazione a più fattori non è supportata, si utilizzano credenziali di elevata robustezza (almeno 14 caratteri) per le utenze da Addetto IT; • se per l'autenticazione si utilizzano certificati digitali viene garantito che le chiavi private siano adeguatamente protette. **[M] 5.7.1** **[M] 5.7.4** **[M] 5.11.1** **[M] 5.11.2**		determina la validità e la relativa gerarchia (Ruoli e permessi) SEP gestisce poi il flusso di approvazione di un utente che faccia richiesta di accedere alla piattaforma a condizione che la validità dell'utente stesso sia confermata dall'LDAP di TIM
CoA-ICT.006.1 CoA-ICT.006.2	Controllo accessi	La piattaforma, o l'eventuale piattaforma centralizzata di Identity Management ad essa connessa, prevede meccanismi automatici di verifica atti a richiedere la sostituzione al primo accesso delle password temporanee inizialmente assegnate a ciascun Addetto IT.	Applicato	Non applicabile in quanto la gestione delle credenziali viene ereditata, tramite collegamento sicuro, dall'LDAP di TIM che ne determina la

Allegato Tecnico di Compliance e Sicurezza – Accordo Quadro RTRT4 - Azienda Regionale Diritto allo Studio Universitario

Emesso da: CE.E.PS/C Data: 30.11.2022

ID MISURA	Categoria MIMIP	Testo requisito	Telsy	OpenSymbol
		[M] 5.11.1		validità e la relativa gerarchia (Ruoli e permessi) SEP gestisce poi il flusso di approvazione di un utente che faccia richiesta di accedere alla piattaforma a condizione che la validità dell'utente stesso sia confermata dall'LDAP di TIM
CoA-ICT.007.1 CoA-ICT.007.2	Controllo accessi	La piattaforma, o l'eventuale piattaforma centralizzata di Identity Management ad essa connessa, prevede meccanismi automatici di verifica atti a richiedere la sostituzione al primo accesso delle password temporanee inizialmente assegnate a ciascun End User Autorizzato. **[M] 5.11.1**	Applicato	Non applicabile in quanto la gestione delle credenziali viene ereditata, tramite collegamento sicuro, dall'LDAP di TIM che ne determina la validità e la relativa gerarchia (Ruoli e permessi) SEP gestisce poi il flusso di approvazione di un utente che faccia richiesta di accedere alla piattaforma a condizione che la validità dell'utente stesso sia confermata dall'LDAP di TIM
CoA-ICT.008.1 CoA-ICT.008.2	Controllo accessi	Per una gestione delle credenziali di autenticazione dedicate a ciascun Addetto IT, la piattaforma, o l'eventuale piattaforma centralizzata di Identity	Applicato	Non applicabile in quanto la gestione delle credenziali viene ereditata, tramite

Allegato Tecnico di Compliance e Sicurezza – Accordo Quadro RTRT4 - Azienda Regionale Diritto allo Studio Universitario

Emesso da: CE.E.PS/C Data: 30.11.2022

ID MISURA	Categoria MIMIP	Testo requisito	Telsy	OpenSymbol
		Management ad essa connessa, prevede meccanismi automatici di verifica atti a richiedere la sostituzione periodica della password almeno ogni 6 mesi e almeno ogni 3 mesi in caso di trattamento di dati sensibili e giudiziari. **[M] 5.7.3**		collegamento sicuro, dall'LDAP di TIM che ne determina la validità e la relativa gerarchia (Ruoli e permessi) SEP gestisce poi il flusso di approvazione di un utente che faccia richiesta di accedere alla piattaforma a condizione che la validità dell'utente stesso sia confermata dall'LDAP di TIM
CoA-ICT.009.1	Controllo accessi	Per una gestione delle credenziali di autenticazione dedicate a ciascun End User Autorizzato al Trattamento, la piattaforma, o l'eventuale piattaforma centralizzata di Identity Management ad essa connessa, prevede meccanismi automatici di verifica atti a richiedere la sostituzione periodica della password almeno ogni 6 mesi nel caso di sistemi che trattano dati personali e almeno ogni 3 mesi in caso di trattamento di dati sensibili e giudiziari.	Applicato	Non applicabile in quanto la gestione delle credenziali viene ereditata, tramite collegamento sicuro, dall'LDAP di TIM che ne determina la validità e la relativa gerarchia (Ruoli e permessi) SEP gestisce poi il flusso di approvazione di un utente che faccia richiesta di accedere alla piattaforma a condizione che la validità dell'utente stesso sia confermata dall'LDAP di TIM

Allegato Tecnico di Compliance e Sicurezza – Accordo Quadro RTRT4 - Azienda Regionale Diritto allo Studio Universitario

Emesso da: CE.E.PS/C Data: 30.11.2022

ID MISURA	Categoria MIMIP	Testo requisito	Telsy	OpenSymbol
CoA-ICT.014.1 CoA-ICT.014.2	Controllo accessi	Per una gestione di base delle credenziali di autenticazione, la piattaforma IT deve essere configurata in modo tale che associ a ciascun Addetto IT un "profilo di autorizzazione" adeguato a garantire l'accesso ai soli dati che sono strettamente necessari per adempiere ai compiti affidati. **[M] 5.1.1**	Applicato	Applicato
Doc-ICT.002.1	Documentazione	Viene garantita l'esistenza di un elenco aggiornato degli eventuali Partner/Fornitori che concorrono all'erogazione del servizio, nella misura in cui effettivamente intervengano nel trattamento dei dati del Cliente. Tale documentazione deve riportare le seguenti informazioni: - identificativo della società esterna; - descrizione sintetica delle responsabilità affidate; - riferimento al contratto di fornitura.	Applicato	Applicato
PdE-ICT.003.1 PdE-ICT.003.2	Protezione degli elaboratori	La piattaforma prevede il corretto funzionamento e aggiornamento del software di protezione antivirus (prevenzione, rilevazione e rimozione virus e malicious code). Per le piattaforme non sincronizzate con l'infrastruttura antivirus aziendale l'aggiornamento deve avvenire con cadenza almeno mensile. **[M] 8.1.1**	Applicato	NA la piattaforma è su hosting evoluto di Opensymbol ma in DC Noovle
PdE-ICT.004.1 PdE-ICT.004.2	Protezione degli elaboratori	Al fine di minimizzare la vulnerabilità della piattaforma e garantire un livello minimo di protezione delle informazioni aziendali nelle piattaforme, sono installati, almeno annualmente, gli	Applicato	Applicato

Allegato Tecnico di Compliance e Sicurezza – Accordo Quadro RTRT4 - Azienda Regionale Diritto allo Studio Universitario

Emesso da: CE.E.PS/C Data: 30.11.2022

ID MISURA	Categoria MIMIP	Testo requisito	Telsy	OpenSymbol
		aggiornamenti del software applicativo (Patch Management).		
PdE-ICT.005.1 PdE-ICT.005.2	Protezione degli elaboratori	Al fine di minimizzare la vulnerabilità della piattaforma e garantire un livello minimo di protezione delle informazioni aziendali nelle piattaforme, sono installati, almeno annualmente, gli aggiornamenti del software di sistema (Patch Management).	Applicato	NA la piattaforma è su hosting evoluto di Opensymbol ma in DC Noovle
PdE-ICT.006.1 PdE-ICT.006.2	Protezione degli elaboratori	Sono state previste attività di configurazione che prevedano la modifica delle impostazioni predefinite del fornitore (ad esempio password, community SNMP, ecc...), l'eliminazione di account e servizi non necessari e la risoluzione delle vulnerabilità di sicurezza note. **[M] 5.3.1**	Applicato	Applicato
PdE-ICT.007.1 PdE-ICT.007.2	Protezione degli elaboratori	Le componenti della piattaforma sono dotate di software per il quale l'azienda ha i diritti di utilizzo	Applicato	Applicato
PdE-ICT.008.1	Protezione degli elaboratori	Tutti i terminali utilizzati per connettersi al sistema prevedono la funzionalità di screensaver con password o in alternativa il sistema abbatte la sessione dopo 15 minuti o, qualora necessario per esigenze operative documentate, di un periodo di inattività limitato entro le 12 ore.	Applicato	NA non richiesto contrattualmente
PdE-ICT.009.1 PdE-ICT.009.2	Protezione degli elaboratori	Per i trattamenti che prevedono l'hosting fisico dei dati all'interno di siti TIM, il sistema risiede all'interno di un Data Center, di un Service Center, di una Centrale o di un sito con equivalente livello di sicurezza fisica. Nel caso di trattamenti in siti di terze parti devono essere previste e	Applicato	Applicato

Allegato Tecnico di Compliance e Sicurezza – Accordo Quadro RTRT4 - Azienda Regionale Diritto allo Studio Universitario

Emesso da: CE.E.PS/C Data: 30.11.2022

ID MISURA	Categoria MIMIP	Testo requisito	Telsy	OpenSymbol
		applicate politiche e misure per stabilire e mantenere il medesimo livello di sicurezza fisica in linea con quanto già previsto dalle policy e procedure aziendali specifiche.		
PdE-ICT.012.1 PdE-ICT.012.2	Protezione degli elaboratori	E' prevista l'adozione di procedure documentabili e/o tecnologie che consentano la gestione sicura e protetta del codice sorgente del programma. Inoltre i codici sorgente non risiedono sui server in esercizio, se non risultano necessari alla normale operatività del sistema.	Applicato	Applicato
Ris-ICT.008.1 Ris-ICT.008.2	Riservatezza	E' prevista la stesura e la corretta implementazione di procedure atte a regolare il processo di cancellazione dei dati del cliente a seguito della cessazione del contratto (ad es. cessazione di qualsiasi obbligazione derivate da accordi contrattuali oppure in applicazione di specifiche normative) assicurando che tali dati vengano cancellati in maniera definitiva e irreversibile al fine di impedire trattamenti non autorizzati degli stessi da parte di Addetti IT o di eventuali altri Clienti. Le tempistiche di cancellazione sono in linea con quanto previsto a livello contrattule.	Applicato	Applicato
Ris-ICT.009.1	Riservatezza	E' garantito l'isolamento logico dei dati relativi a clienti differenti su una medesima piattaforma. In particolare non deve essere possibile accedere/visualizzare i dati di un Cliente diverso da quello che ha acceduto alla piattaforma.	Applicato	Applicato

ID MISURA	Categoria MIMIP	Testo requisito	Telsy	OpenSymbol
Ris-ICT.010.1	Riservatezza	E' prevista la separazione degli ambienti dedicati alle attività di sviluppo, test e collaudo dall'ambiente di esercizio della piattaforma. Per gli ambienti diversi da quello di produzione nel caso vengano utilizzati dati reali di esercizio, sono garantiti tutti i requisiti di compliance previsti.	Applicato	Applicato
Ris-ICT.011.1	Riservatezza	E' prevista la redazione formale di apposite procedure di estrazione o trasmissione dei dati trattati dalla piattaforma. Tali estrazioni/trasmissioni devono consentire la portabilità dei dati tramite l'esportazione degli stessi in formati standard in relazione alla tecnologia utilizzata (ad es. sistemi di tipo UNIX) e al layer di trattamento (ad es. DB).	Applicato	Applicato

2.2. Perimetro Pubbliche Amministrazioni (Misure Agid)

Ad aprile 2017 AgiD ha pubblicato nella Gazzetta Ufficiale (GuRI) le Misure Minime di Sicurezza per la PA, un documento che contiene le Misure minime di sicurezza ICT per le Pubbliche Amministrazioni le quali costituiscono parte integrante delle Linee Guida per la sicurezza ICT delle Pubbliche Amministrazioni.

Le misure minime Agid sono indicate con la nomenclatura ABSC (Agid Basic Security Controll), cioè con identificatore gerarchico a tre livelli x,y.z preceduti dalla lettera M per indicare la misura come minima (**[M].x.y.z**).

L'appartenenza di una piattaforma a tale perimetro prevede necessariamente l'inclusione della stessa anche all'interno del Perimetro 231/01 reati informatici e del Perimetro Dati Personali.

ID MISURA	Categoria MIMIP	Testo requisito	Telsy	OpenSymbol
PdE-ICT.013.1	Protezione degli elaboratori	E' previsto che venga applicata una protezione crittografica sui dati rilevanti (aventi particolari requisiti di riservatezza). Per le soluzioni custom	Applicato	NA si trattano solo dati comuni (nome,

Allegato Tecnico di Compliance e Sicurezza – Accordo Quadro RTRT4 - Azienda Regionale Diritto allo Studio Universitario

Emesso da: CE.E.PS/C Data: 30.11.2022

ID MISURA	Categoria MIMIP	Testo requisito	Telsy	OpenSymbol
PdE-ICT.013.2		condividere contrattualmente con il cliente quali sono i dati rilevanti. **[M] 13.1.1**		cognome, mail e telefono)
Doc-ICT.012.1	Documentazione	E' prevista l'implementazione di un inventario delle risorse di tutti i sistemi collegati alla rete e dei dispositivi di rete stessi, che registra almeno l'indirizzo IP, da aggiornare quando nuovi dispositivi approvati vengono collegati in rete. **[M] 1.1.1** **[M] 1.3.1** **[M]1.4.1** **[M]1.4.1**	Applicato	NA non richiesto contrattualmente. L'accesso avviene tramite autenticazione su LDAP TIM
PdE-ICT.014.1	Protezione degli elaboratori	E' prevista la redazione di un elenco di software autorizzati, con relative versioni, necessari per ciascun tipo di sistema, compresi server e al contempo non è consentita l'installazione di software non compreso in tale elenco. E' prevista l'esecuzione di regolari scansioni sui sistemi al fine di rilevare la presenza di software non autorizzato. [**M] 2.1.1** **[M] 2.3.1**	Applicato	NA non previsto contrattualmente
Bck-ICT.004.1	Back-up	Su server e per la protezione dei sistemi operativi, sono definite, impiegate e ripristinate (nel caso vengano compromessi) configurazioni standard. Le immagini d'installazione sono memorizzate offline. **[M] 3.1.1** **[M] 3.1.1** **[M] 3.2.1** **[M] 3.2.2** **[M] 3.3.1**	Applicato	NA la piattaforma è su hosting evoluto di Opensymbol ma in DC Noovle
PdE-ICT.015.1	Protezione degli elaboratori	E' assicurato che gli strumenti di scansione delle vulnerabilità (anche per i sistemi separati dalla rete) siano regolarmente aggiornati adottando misure di sicurezza adeguate al livello di criticità. Inoltre è periodicamente verificato che le vulnerabilità emerse dalle scansioni siano state risolte, documentando e accettando in caso opposto un ragionevole rischio. A ciascuna azione utile per la risoluzione delle vulnerabilità è assegnato un livello di priorità in base al rischio associato. Ad ogni modifica significativa della configurazione deve essere eseguita la	Applicato	NA la piattaforma è su hosting evoluto di Opensymbol ma in DC Noovle

Allegato Tecnico di Compliance e Sicurezza – Accordo Quadro RTRT4 - Azienda Regionale Diritto allo Studio Universitario

Emesso da: CE.E.PS/C Data: 30.11.2022

ID MISURA	Categoria MIMIP	Testo requisito	Telsy	OpenSymbol
		ricerca delle vulnerabilità con strumenti automatici che forniscano report con indicazioni delle vulnerabilità più critiche. **[M] 4.1.1** **[M] 4.4.1** **[M] 4.5.2** **[M] 4.7.1** **[M] 4.8.2**		
PdE-ICT.016.1	Protezione degli elaboratori	Vengono scaricati automaticamente e installati le patch e gli aggiornamenti del software di sistema operativo necessari a correggere difetti e prevenire vulnerabilità della piattaforma. L'installazione avviene automaticamente qualora non preveda un'interruzione o una forte limitazione dell'operatività. In particolare sono applicate le patch per le vulnerabilità a partire da quelle più critiche. **[M] 4.5.1** **[M] 4.7.1** **[M] 4.8.2**	Applicato	NA la piattaforma è su hosting evoluto di Opensymbol ma in DC Noovle
PdE-ICT.017.1	Protezione degli elaboratori	Vengono scaricati automaticamente e installati le patch e gli aggiornamenti del software di DBMS e applicativo oggetto del SaaS, necessari a correggere difetti e prevenire vulnerabilità della piattaforma. L'installazione avviene automaticamente qualora non preveda un'interruzione o una forte limitazione dell'operatività. In particolare sono applicate le patch per le vulnerabilità a partire da quelle più critiche. **[M] 4.5.1** **[M] 4.7.1** **[M] 4.8.2**	Applicato	NA la piattaforma è su hosting evoluto di Opensymbol ma in DC Noovle
CoA-ICT.015.1	Controllo accessi	Vengono completamente distinte utenze privilegiate e non privilegiate degli amministratori (alle quali devono corrispondere credenziali diverse), mentre è consentito l'utilizzo delle utenze amministrative anonime (ad esempio “root” di UNIX o “Administrator” di Windows) solo per le situazioni di emergenza; queste vengono gestite in modo da garantire la disponibilità e la riservatezza e in modo da assicurare l’imputabilità di chi ne fa uso.	Applicato	NA non richiesto contrattualmente

Allegato Tecnico di Compliance e Sicurezza – Accordo Quadro RTRT4 - Azienda Regionale Diritto allo Studio Universitario

Emesso da: CE.E.PS/C Data: 30.11.2022

ID MISURA	Categoria MIMIP	Testo requisito	Telsy	OpenSymbol
		[M] 5.10.1 **[M] 5.10.3**		
PdE-ICT.018.1	Protezione degli elaboratori	Sulle piattaforme non sono consentite l'esecuzione automatica dei contenuti, dinamici e non, e l'anteprima automatica dei contenuti dei file, anche al momento della connessione dei dispositivi removibili e l'apertura automatica dei messaggi di posta elettronica. Limitare l'uso di dispositivi esterni a quelli necessari per le attività aziendali. **[M]8.3.1** **[M] 8.7.1** **[M] 8.7.2** **[M] 8.7.3** **[M] 8.7.4:**	Applicato	NA non richiesto contrattualmente
PdE-ICT.019.1	Protezione degli elaboratori	Qualsiasi supporto removibile utilizzato è automaticamente soggetto ad una scansione anti-malware, inoltre sono adottati e configurati adeguati strumenti di web filtering e nel caso di posta elettronica antispamming bloccando nella posta elettronica e nel traffico web i file potenzialmente pericolosi la cui tipologia non è strettamente necessaria per l'organizzazione. **[M] 8.8.1** **[M] 8.9.1** **[M] 8.9.2** **[M] 8.9.3**	Applicato	NA non richiesto contrattualmente
CdC-ICT.013.1	Canali di comunicazione	Le operazioni di amministrazione remota di server, dispositivi di rete e analoghe apparecchiature sono eseguite per mezzo di connessioni protette (protocolli intrinsecamente sicuri, ovvero su canali sicuri). **[M] 3.4.1**	Applicato	Applicato
CdC-ICT.014.1	Canali di comunicazione	E' prevista la possibilità di bloccare il traffico da e verso url presenti in una blacklist. **[M] 13.8.1**	Applicato	NA la piattaforma è su hosting evoluto di Opensymbol ma in DC Noovle
Ris-ICT.013.1	Riservatezza	Risulta garantita l'applicazione delle misure di sicurezza derivanti dalle analisi del rischio (Piano di Sicurezza) relative alla piattaforma a supporto del servizio erogato. **[M] 4.8.1**	Applicato	Applicato

2.3. Perimetro Portali Web

Composto dalle piattaforme che realizzano Portali / Siti web che utilizzano cookies per la navigazione libera di utenti generici attraverso l'utilizzo dei browser HTTP di navigazione Internet.

I cookie (file di informazioni che i siti web memorizzano sul computer dell'utente di Internet durante la navigazione), si suddividono in:

- Cookie Tecnici – Necessari per effettuare la navigazione in rete o per fornire servizi esplicitamente richiesti dall'utente, sono da considerarsi cookie tecnici, i cookie di autenticazione (utili anche per mantenere attiva la connessione ad aree riservate durante la navigazione attraverso le pagine del sito senza la necessità di reinserire User-Id e password), quelli di sicurezza (numero di login falliti), funzionali (utilizzati per memorizzare informazioni specifiche riguardanti gli utenti stessi, tra cui le preferenze, come ad esempio la lingua, il tipo di browser e di computer usato, il contenuto del "carrello della spesa"), per bilanciare le richieste utente, di sessione (per migliorare la fruibilità del sito), per la gestione dei contenuti multimediali (per archiviare dati tecnici);
- Cookie di Profilazione – Monitorano il comportamento degli utenti durante la navigazione in rete al fine creare profili relativi all'utente (sui suoi gusti, abitudini, scelte, ecc.) e vengono utilizzati soprattutto al fine di inviare messaggi pubblicitari personalizzati;
- Cookie analytics (analitici) – Utilizzati per rilevare a livello statistico gli utenti unici e su come hanno visitato il sito. Sono assimilati ai cookie tecnici laddove utilizzati direttamente dal gestore del sito (di prima parte) ed utilizzati solo per la suddetta finalità; a queste condizioni, sono detti cookie analytics di "prima parte" per i quali valgono le stesse regole previste per i cookie tecnici (cioè è sufficiente l'informativa). Invece, per i cookie analytics di "terze parti" (es. Google analytics) è necessario fornire l'informativa e raccogliere il consenso dell'utente; il consenso non necessario solo se sono adottati strumenti che riducono il potere identificativo (anonimizzazione anche parziale dell'IP dell'internauta del cookie) e la terza parte garantisce che non incrocia le informazioni con altre di cui già dispone.

L'appartenenza di una piattaforma a tale perimetro prevede necessariamente l'inclusione della stessa anche all'interno del Perimetro 231/01 reati informatici e del Perimetro Dati Personali.

ID MISURA	Categoria Mimip	Testo requisito	Opensymbol

Allegato Tecnico di Compliance e Sicurezza – Accordo Quadro RTRT4 - Azienda Regionale Diritto allo Studio Universitario

Emesso da: CE.E.PS/C Data: 30.11.2022

AuL-ICT.019.1	Audit log	Nel caso in cui il portale web consenta l'invio di cookie di profilazione di prima parte, TIM, in qualità di gestore del sito, individua e implementa misure idonee al fine di: - tracciare l'avvenuta prestazione del consenso dell'utente relativo ai cookie di profilazione di prima parte, anche mediante l'eventuale utilizzo di un «cookie tecnico» ad hoc, anche al fine di evitare di riproporre l'informativa breve alla seconda visita del medesimo utente sullo stesso sito; - consentire all'utente di poter modificare le proprie scelte (cioè modificare il consenso ai cookie di profilazione di prima parte) accedendo all'informativa estesa (ad esempio ad un "pannello" ad hoc). Per i cookie di profilazione di terze parti ed i cookie analytics di terze parti, ospitati sul portale web del Cliente, i suddetti adempimenti sono a cura delle terze parti.	Applica per i cooki tecnici.
Ris-ICT.016.1	Riservatezza	Nel caso in cui il portale web consenta l'invio, oltre ai cookie tecnici, di cookie di profilazione (di prima o di terze parti) o di analytics di terze parti (senza anonimizzazione, anche parziale, o cancellazione dell'IP dell'internauta), il portale è sviluppato in maniera tale da prevedere funzionalità volte a garantire la presenza in primo piano di un banner rivolto all'utente finale recante l'informativa «breve» e la richiesta di consenso relativa all'utilizzo dei cookie. Tale banner costituisce una percettibile discontinuità nella fruizione dei contenuti della pagina web e contiene le seguenti informazioni: a) che il sito utilizza cookie di profilazione al fine di inviare messaggi pubblicitari in linea con le preferenze manifestate dall'utente nell'ambito della navigazione in rete; b) che il sito consente l'invio anche di cookie di terze parti (qualora avvenga); c) un link che rimanda all'informativa estesa; d) l'indicazione che alla pagina dell'informativa estesa è possibile negare il consenso all'installazione di qualunque cookie; e) l'indicazione che la prosecuzione della navigazione mediante accesso ad altra area del sito o selezione di un elemento dello stesso comporta la prestazione del consenso all'uso dei cookie.	Non applicato, non sono inviati cookie di profilazione
Ris-ICT.017.1	Riservatezza	Il portale web è sviluppato in maniera tale da rendere raggiungibile l'informativa estesa, attraverso un riferimento su ogni pagina del sito / portale, collocato in calce allo stesso e, ove previsto (nel caso in cui il portale web consente l'invio, oltre ai cookie tecnici, di cookie di profilazione o di analytics di terze parti), da un link presente nel banner di informativa breve. L'informativa «estesa» è sempre predisposta indipendentemente dalla finalità dei cookie (tecnici, di profilazione e di analytics).	Non applicabile in quanto non vengono inviati cookie di analytics
Ris-ICT.018.1	Riservatezza	Il portale web è sviluppato in maniera tale che l'informativa estesa possa contenere le seguenti informazioni: - indicazioni sull'uso di cookie tecnici, di profilazione e di analytics; - possibilità di scegliere quali specifici cookie autorizzare; - possibilità per l'utente di manifestare le proprie opzioni in merito all'uso dei cookie anche tramite le impostazioni del browser, indicando la procedura per configurare tali impostazioni; - i link aggiornati alle informative ed ai moduli di consenso relativi ai cookie di terze parti presenti nel sito (inclusi i link di eventuali soggetti intermediari).	Non applicabile in quanto non vengono inviati cookie di analytics
Ris-ICT.019.1	Riservatezza	La scadenza dei cookie di profilazione di prima parte è impostata ad un periodo massimo di 12 mesi.	Non applicabile in quanto non vengono inviati cookie di profilazione

CHIANTINI SONIA 12.12.2022 07:54:53 GMT+01:00

Firmato digitalmente da: STEFANO CINQUINI
TIM S.p.A.
Firmato il 01/12/2022 18:45
Seriale Certificato: 446471
Valido dal 18/03/2021 al 17/03/2024
TI Trust Technologies CA